Latimeria chalumnae

Anto Veldre

anto.veldre

anto ät xyz.ee

Danske Bank

Sampo Pank

http://en.wikipedia.org/wiki/Latimeria

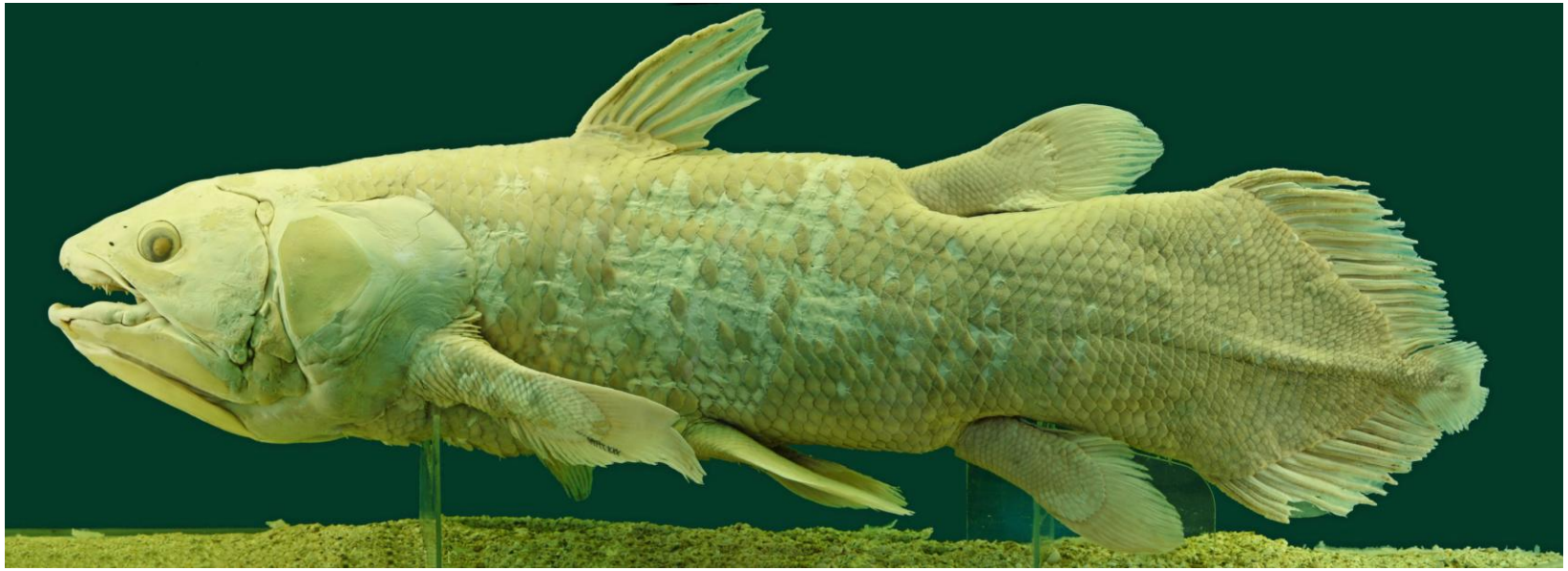
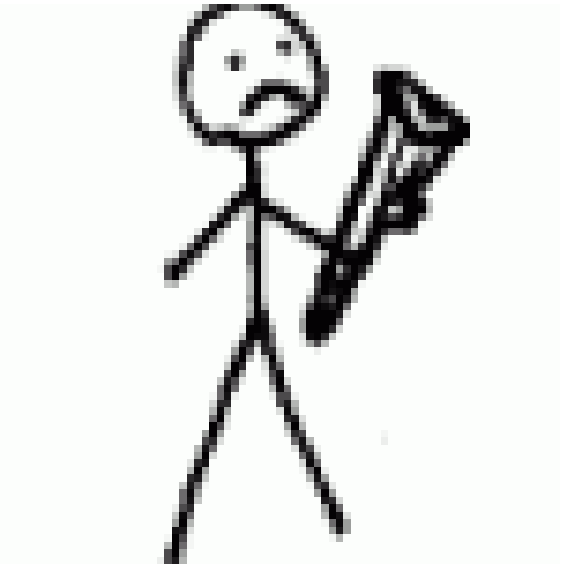


Photo: Wikipedia

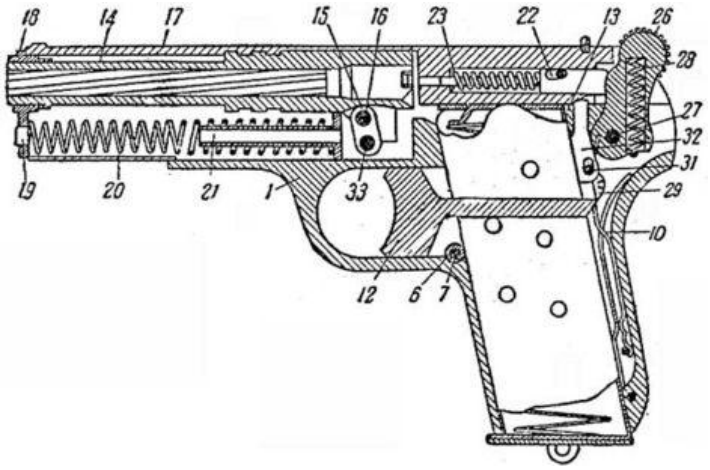
A.B.



- Age 43, male
- Profession: electrician
- Hobbies: guns, reading i386 asm books

Episode 1

- Approx 2002
- Illegal possession and carrying of a handgun
- Convicted, served



Episode 2

- Buying a computer
- Launching DoS
- R-admin vulnerability
- IP hardcoded into
- No CCC
- No propagation
- UDP flood

29-30 July 2004

MS04-012

- 0,00, 000,0000,00000,000000,0000000,00000000, 1,12,123,1234,12345,123456,1234567,12345678,1234567 89,abc123,access,adm,Admin.alpha,anon,anonymous,asdf gh backdoor,backup,beta,bin, coffee,computer,crew, database,debug,default,demo go,guest hello install,internet, login,mail,manager,money,monitor,network,new,newpass, nick,nobody,nopass,oracle,pass,passwd,password,poiuytre, private,public qwerty, random,real,remote,root,ruler secret, secure, security, server, setup, shadow, shit, sql, super, sys, system,telnet, temp, test, test1, test2, visitor, windows,www, X

Episode 3

photo: margo@blogspot

- ISP, cable operator
- Episode 1 investigation, src IP was noted up
- DNS servers, DHCP server attacked
- Manually crafted

May ? 2006

Episode 4

Early June 2006

- DDoS against Starman
- Propagation capabilities
- Target www . starman . ee
  - hardcoded into binary
- UDP flood, HTTP get
- 100-200 Mbit/sec

Episode 5

Photo: NCC

14. August 2007

- Insurance company IF
- A car accident
  - Driving drunk
  - Another person without a driving license involved
- DDoS since then
- 2007-11-06 100 Mbit/sec

Allaple virus

- "Backdoor.Win32.Allaple "
- "Trojan.Starman"
- Microsoft: Worm:Win32/Rahack.A

- "GET / HTTP/1.1\r\n“

- http://blogs.securiteam.com/index.php/archives/856
- http://isc.sans.org/diary.html?storyid=2451

Allaple virus

- Several versions
- 1-3 WWW servers targeted (2x if + starman)
- Payload:
  - HTTP GET
  - echo requests
  - TCP SYN
  - ICMP "Babcdefghijklmnopqrstuvwabcdefghi“
- Propagation:
  - Scan for R-admin, misuse MS04-012
- Polymorphism due to IP scan range bytes

Aftermath

- A.B. not yet convicted.
  - was in custody till February 2008
  - currently waiting for court
- Finnisch CERT analysis
  - DDoS Microlink radminned code + propagation routines = Allaple

Estonian Penal Code

§ 206. Computer sabotage

- (1) Unlawful replacement, deletion, damaging or blocking of data or programs in a computer, if significant damage is thereby caused, or unlawful entry of data or programs in a computer, if significant damage is thereby caused, is punishable by a pecuniary punishment or up to one year of imprisonment.

- (2) The same act, if **committed with the intention to interfere with the work of a computer or telecommunications system, is punishable by a pecuniary punishment or up to 3 years'** imprisonment.

Happy end?

- *Latimeria chalumnae*

100 MBit/sec DDoS

Thnx!